

# NATAS Write-up (L0 -L10)

Natas teaches the basics of server-side web security, available on [overthewire.org](https://overthewire.org)

Natas is a series of web security training levels hosted on the OverTheWire website. It's designed to teach fundamental server-side web security concepts through a series of challenges. Each level involves a website with hashtag#vulnerabilities, and the goal is to exploit them to find the password for the next level.

Each level of Natas consists of its website located at <http://natasX.natas.labs.overthewire.org>, where X is the level number. There is no SSH login. To access a level, enter the username for that level (e.g. natas0 for level 0) and its password.

Each level has access to the password of the next level. Your job is to somehow obtain that next password and level up. All passwords are also stored in /etc/natas\_webpass/. E.g. The password for natas5 is stored in the file /etc/natas\_webpass/natas5 and is only readable by natas4 and natas5.

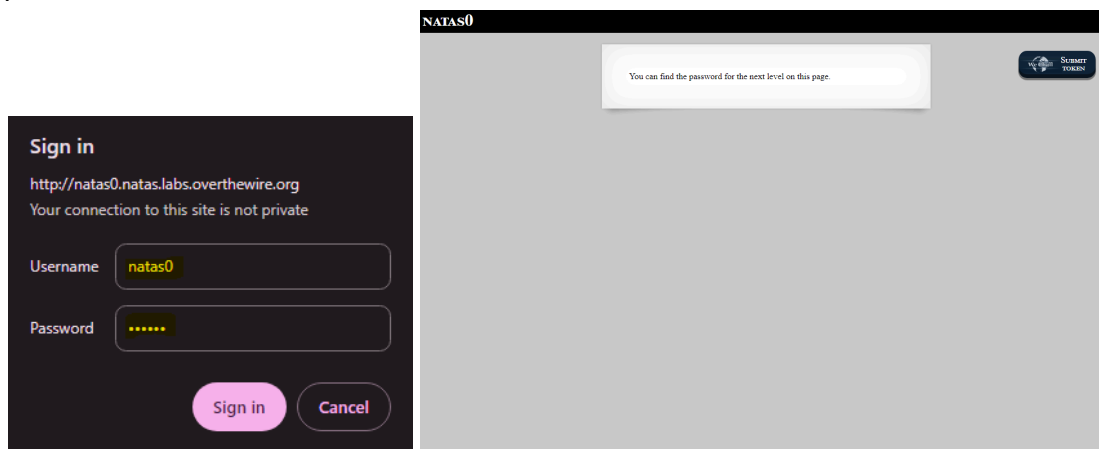
## Level 0:

**Username: natas0**


**Password: natas0**

**URL: <http://natas0.natas.labs.overthewire.org>**

Now go to the URL, a sign-up popup will appear, enter the username and password, provided above.



First let's check what the “*Submit Token*” button is:



# We Chall

**English** ▾ **News** **Links** **Sites** **Forum** **Ranking** **Challenges** **Downloads** **Register**

**New Sites**

pwn.college  
PWN.TN  
PromptRiddle  
PyDéfis

CryptoHack  
247CTF  
Énigmes À Thématiques  
LordofSQLi

**New Users**

c0d3m0n  
MRX1  
hab  
Leiyas

br202  
vorr3x  
jenni\_purr  
majd

**31 Online**  
Guest(x26), c0d3m0n, cup\_of\_tea, hab, tehran

**GWF**

✖ For this function you need to be logged in.

English ▾

Slovak ▾

Spanish ▾

French ▾

German ▾

Korean ▾

Polish ▾

Cracking ▾

Crypto ▾

Exploit ▾

Flash ▾

Forensic ▾

IRC ▾

Java ▾

JavaScript ▾

LockPicking ▾

Logic ▾

Math ▾

MySQL ▾

Programming ▾

Realistic ▾

Research ▾

Reversing ▾

Science ▾

Shell ▾

Stegano ▾

Storyline ▾

Warbox ▾

Web ▾

Natas ▾

Details

WarBoxes

Ranking

History

All Sites

Active Sites

Graveyard


Not Ranked


Coming Soon

**Levels for the Natas box on OverTheWire.org**

There are currently 35 levels available on the Natas box on OverTheWire.org. Please note that on ssh wargames the levels are added when they get solved the first time.

Pos	Score	Title	Solvers	LastSolvedBy	LastSolved
0	0	<a href="#">natas0</a>	10981	<a href="#">andersfv</a>	Jul 18, 2024 - 11:22:18
1	1	<a href="#">natas1</a>	9582	<a href="#">bluekafka</a>	Jun 09, 2024 - 00:00:34
2	1	<a href="#">natas2</a>	9181	<a href="#">bluekafka</a>	Jun 09, 2024 - 00:01:15
3	1	<a href="#">natas3</a>	8015	<a href="#">tammy</a>	Jun 08, 2024 - 16:51:22
4	1	<a href="#">natas4</a>	7243	<a href="#">bluekafka</a>	Jun 09, 2024 - 08:03:02
5	1	<a href="#">natas5</a>	6293	<a href="#">ted1337</a>	Jun 06, 2024 - 23:37:11
6	1	<a href="#">natas6</a>	5853	<a href="#">ted1337</a>	Jun 06, 2024 - 23:38:46
7	1	<a href="#">natas7</a>	5705	<a href="#">ted1337</a>	Jun 06, 2024 - 23:42:33
8	1	<a href="#">natas8</a>	5530	<a href="#">ted1337</a>	Jun 06, 2024 - 23:47:51
9	1	<a href="#">natas9</a>	5305	<a href="#">ted1337</a>	Jun 06, 2024 - 23:59:10
10	1	<a href="#">natas10</a>	4954	<a href="#">ted1337</a>	Jun 06, 2024 - 23:59:44
11	1	<a href="#">natas11</a>	4451	<a href="#">ted1337</a>	Jun 07, 2024 - 01:51:03
12	1	<a href="#">natas12</a>	3390	<a href="#">heyimsudo</a>	Jun 08, 2024 - 23:04:57
13	1	<a href="#">natas13</a>	2980	<a href="#">ted1337</a>	Jun 09, 2024 - 01:48:35
14	1	<a href="#">natas14</a>	2833	<a href="#">ted1337</a>	Jun 09, 2024 - 01:50:59

**Signup** 



Restrict session to IP ☒

[Login](#)

[Register](#) [Forgot password](#)

**Statistics**

47 Sites  
182 Challs  
8945 Posts  
67118 Users  
41 donations  
0 Patreons  
1 Shop

**47 Active Sites**

World of Wargame  
WeChall  
TheBlackSheep  
Rankk  
Electrica  
NewbieContest  
LOST-Chall  
Yashira  
BrainQuest  
Net-Force  
HackThisSite  
ThisIsLegal.com  
elhacker.net  
TryThisOne  
TDHack  
+Ma's Reversing

That's nothing useful for now.

Now let's inspect the page:

The screenshot displays a web browser window with the URL `https://www.wechall.net/18-levels-on-Natas.html`. The browser's developer tools are open, showing the 'Elements' panel on the left and the 'Styles' panel on the right. The 'Elements' panel shows the HTML structure of the page, including a `<form>` element with the action `https://www.wechall.net/18-levels-on-Natas.html`. The 'Styles' panel shows the styles applied to the `form` element, including `display: none;` and `background-color: #f0f0f0;`. The form itself is a 'realwechallform' with fields for 'email', 'password\_solution', and 'password\_register'. The form is styled with a light blue background and a white border. The 'password\_solution' field is highlighted in yellow. The 'password\_register' field is highlighted in light blue. The form is submitted to the URL `https://www.wechall.net/18-levels-on-Natas.html`.

There's also nothing useful.

Now let's check the page source:

```
view-source:natas0.natas.labs.overthewire.org
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
10 <script>var wechallinfo = { "level": "natas0", "pass": "natas0" };</script></head>
11 <body>
12 <h1>natas0</h1>
13 <div id="content">
14 You can find the password for the next level on this page.
15
16 <!--The password for natas1 is 0nzcigAq7t2iALyvU9xcHlYN4MlkIwlq -->
17 </div>
18 </body>
19 </html>
20
21
```

We got the first one: **0nzcigAq7t2iALyvU9xcHlYN4MlkIwlq.**

## Level 0 → Level 1:

**Username: natas1**

**URL: <http://natas1.natas.labs.overthewire.org>**

Go to the URL and enter the username “*natas1*” and the password we got on the last level.

The image shows a 'Sign in' form for the URL <http://natas1.natas.labs.overthewire.org>. A warning message states 'Your connection to this site is not private'. The form has two input fields: 'Username' with the value 'natas1' and 'Password' with a masked password represented by dots. At the bottom are 'Sign in' and 'Cancel' buttons.

You can find the password for the next level on this page, but rightclicking has been blocked!



*You can find the password for the next level on this page, but right-clicking has been blocked!*

So in this, we can't interact with the page, which means we can't get to the page source because the flag must be hidden there. So now let's play with URLs.

As we need to get the page source, so just add "view-source:" at the start of the URL.

```

view-source:
<html>
<head>
  <!-- This stuff in the header has nothing to do with the level -->
  <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
  <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
  <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
  <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
  <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
  <script src="http://natas.labs.overthewire.org/js/wechall_data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
  <script>var wechallinfo = { "level": "natas1", "pass": "0nzcip4q7t2iaLyvU9xchLYM4Hk1q" };</script></head>
  <body oncontextmenu="javascript:alert('right clicking has been blocked');return false;">
  <h1>natas1</h1>
  <div id="content">
    You can find the password for the
    next level on this page, but rightclicking has been blocked!

    <!--The password for natas2 is TguMNxKo1DSa1tujBLuZJnDU1CcUAP1I -->
  </div>
</body>
</html>

```

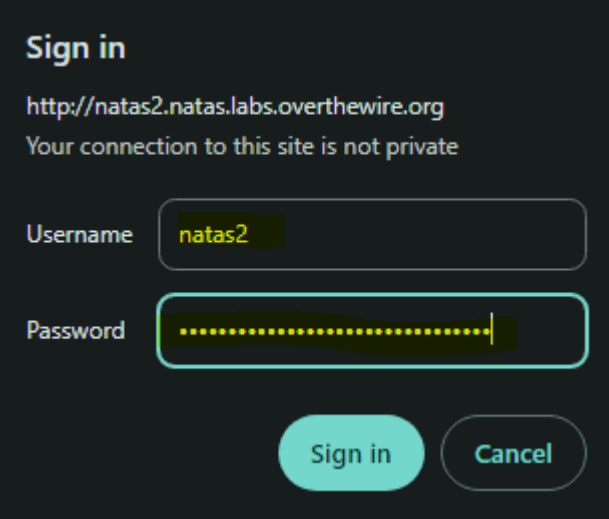
We got the second one: **TguMNxKo1DSa1tujBLuZJnDU1CcUAP1I**

## Level 1 → Level 2:

Username: **natas2**

URL: **http://natas2.natas.labs.overthewire.org**

Go to URL:



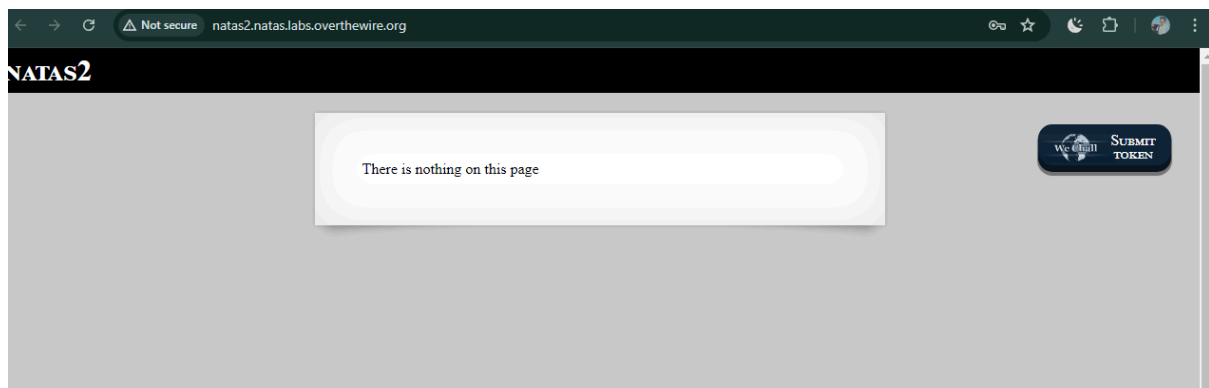
Sign in

<http://natas2.natas.labs.overthewire.org>

Your connection to this site is not private

Username

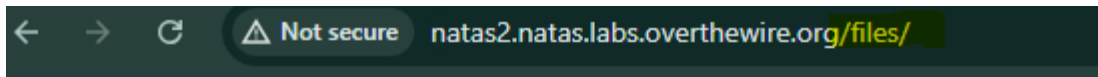
Password






Let's again go to view source:

```
Line wrap
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
10 <script>var wechallinfo = { "level": "natas2", "pass": "TguMwXKo1DSaltuj8LUzJnDULccUAP1I" };</script></head>
11 <body>
12 <h1>natas2</h1>
13 <div id="content">
14 There is nothing on this page
15 
16 </div>
17 </body></html>
18
```

It reveals that there is another page with the name *"file"*. Let's get there:



## Index of /files

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">pixel.png</a>	2024-07-17 15:52	303	
 <a href="#">users.txt</a>	2024-07-17 15:52	145	

Apache/2.4.58 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCxkVV3m
natas3:3gqisGdR0pjm6tpkDKdIW02hSvchLeYH
eve:zo4mJWyNj2
mallory:9urtcpzBmH
```

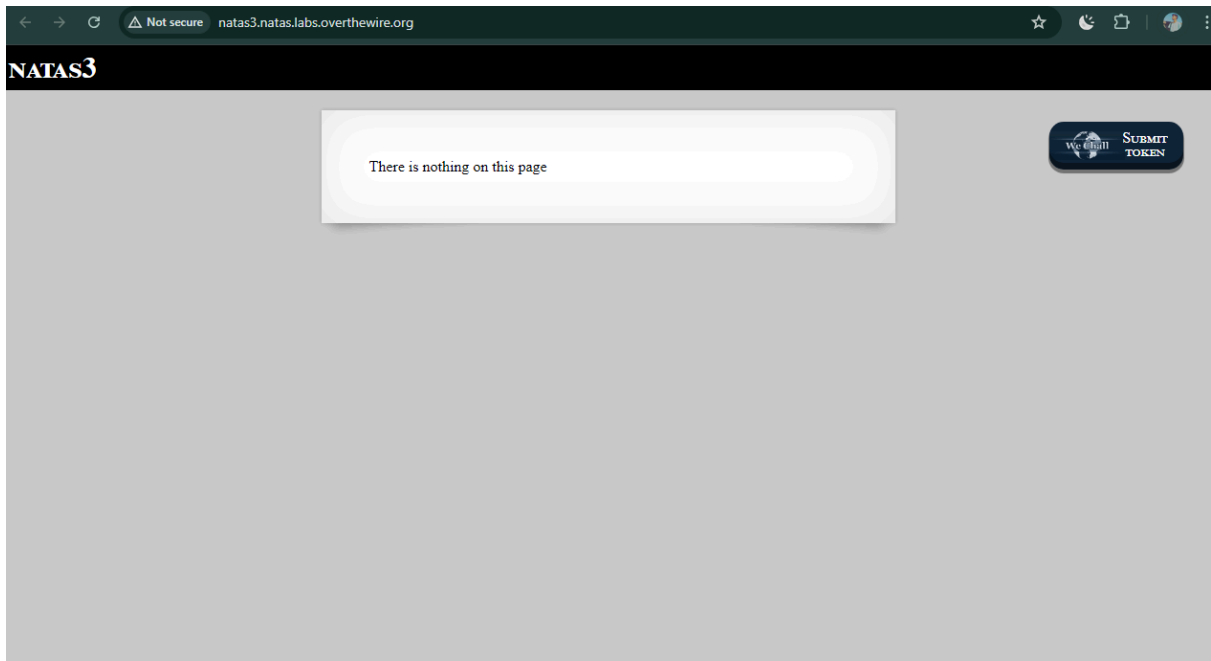
Here is the third one: **3gqisGdR0pjm6tpkDKdIW02hSvchLeYH**

## Level 2 → Level 3:

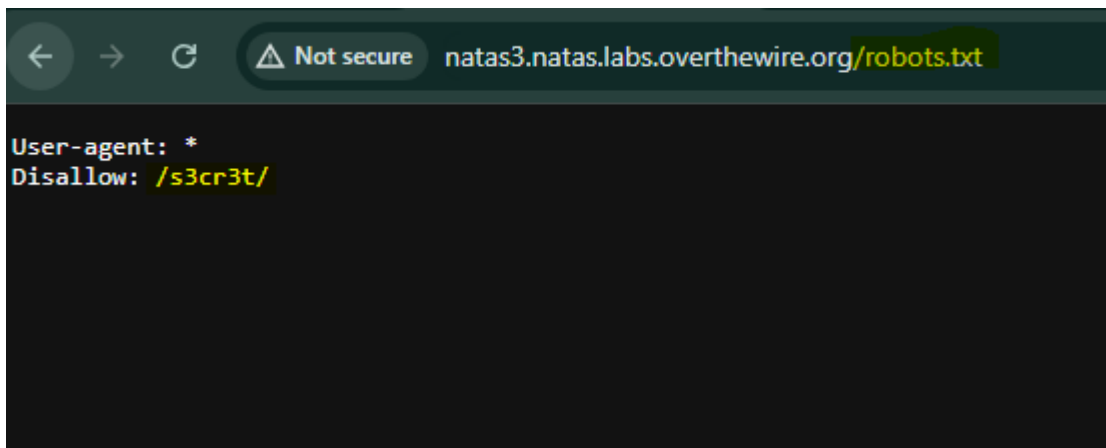
**Username: natas3**

**URL: http://natas3.natas.labs.overthewire.org**

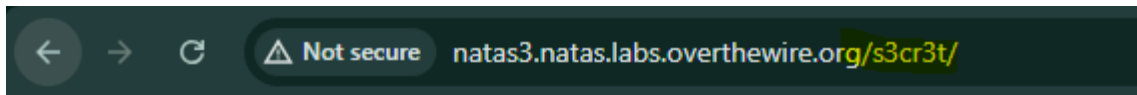
Go to URL, enter username and password from the last level:




With little research, I came to know that search engines sometimes crawl the website, which is a process used by engines to discover and index the content of the websites. This also leaves with the new index “*robots.txt*”.



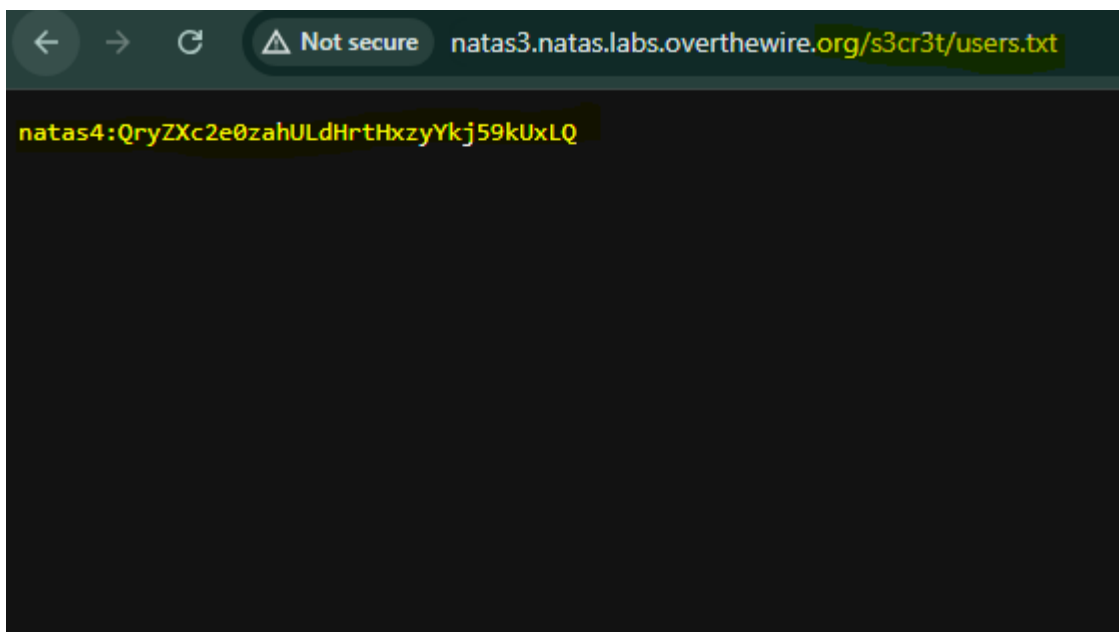
So it says that an index with that name is disallowed. Let's get there:



## Index of /s3cr3t

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">users.txt</a>	2024-07-17 15:52	40	

Apache/2.4.58 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80



Here is another: `QryZXc2e0zahULdHrtHxzyYkj59kUxLQ`

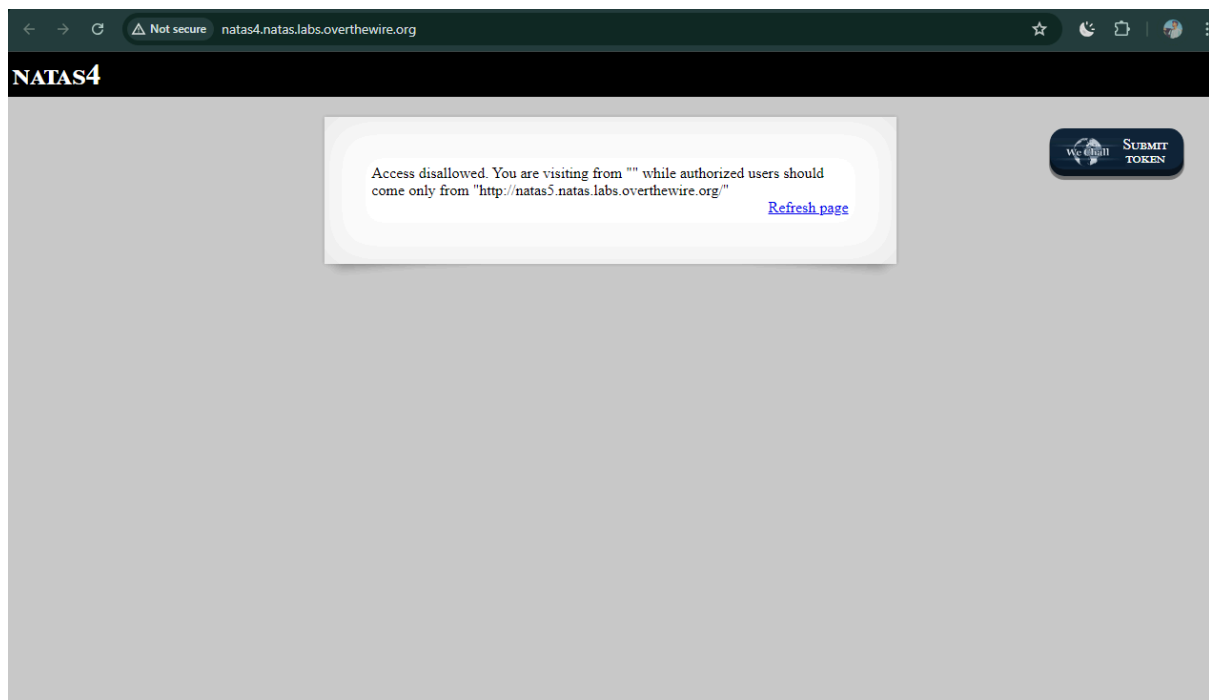
## Level 3 → Level 4:

Username: `natas4`

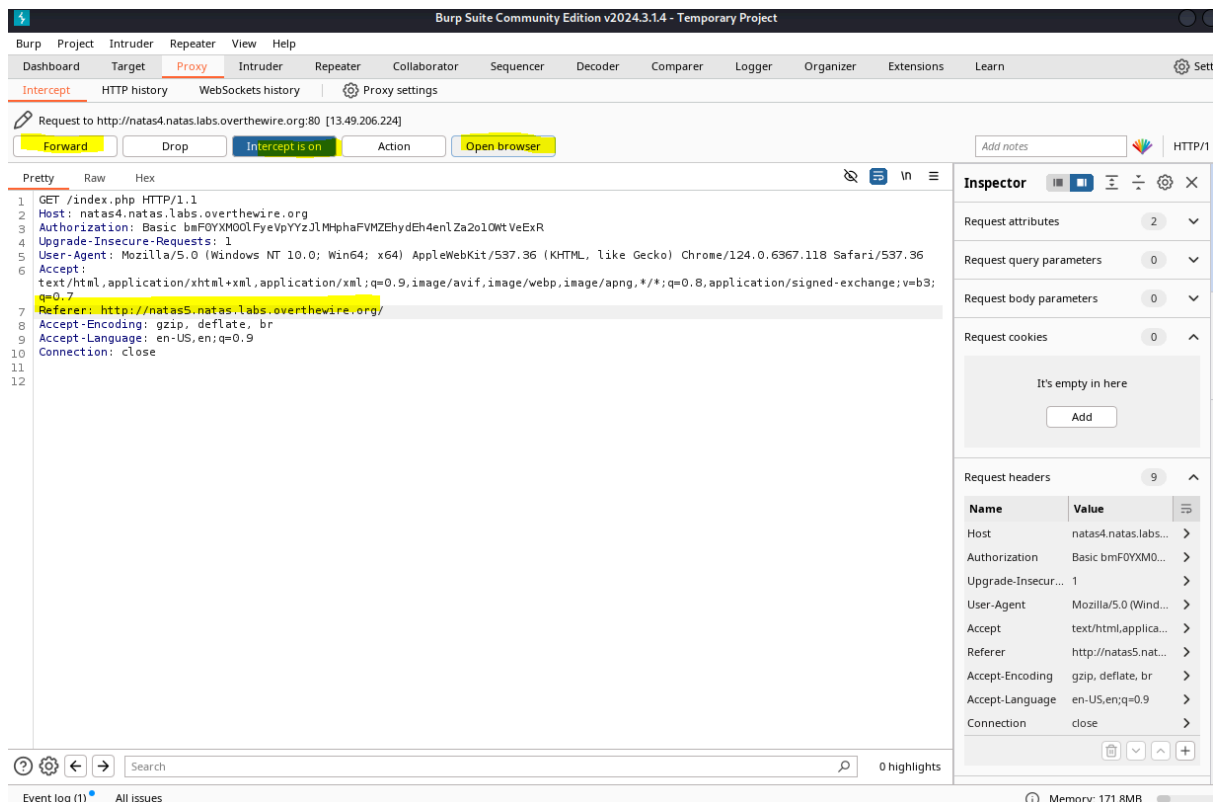
URL: `http://natas4.natas.labs.overthewire.org`



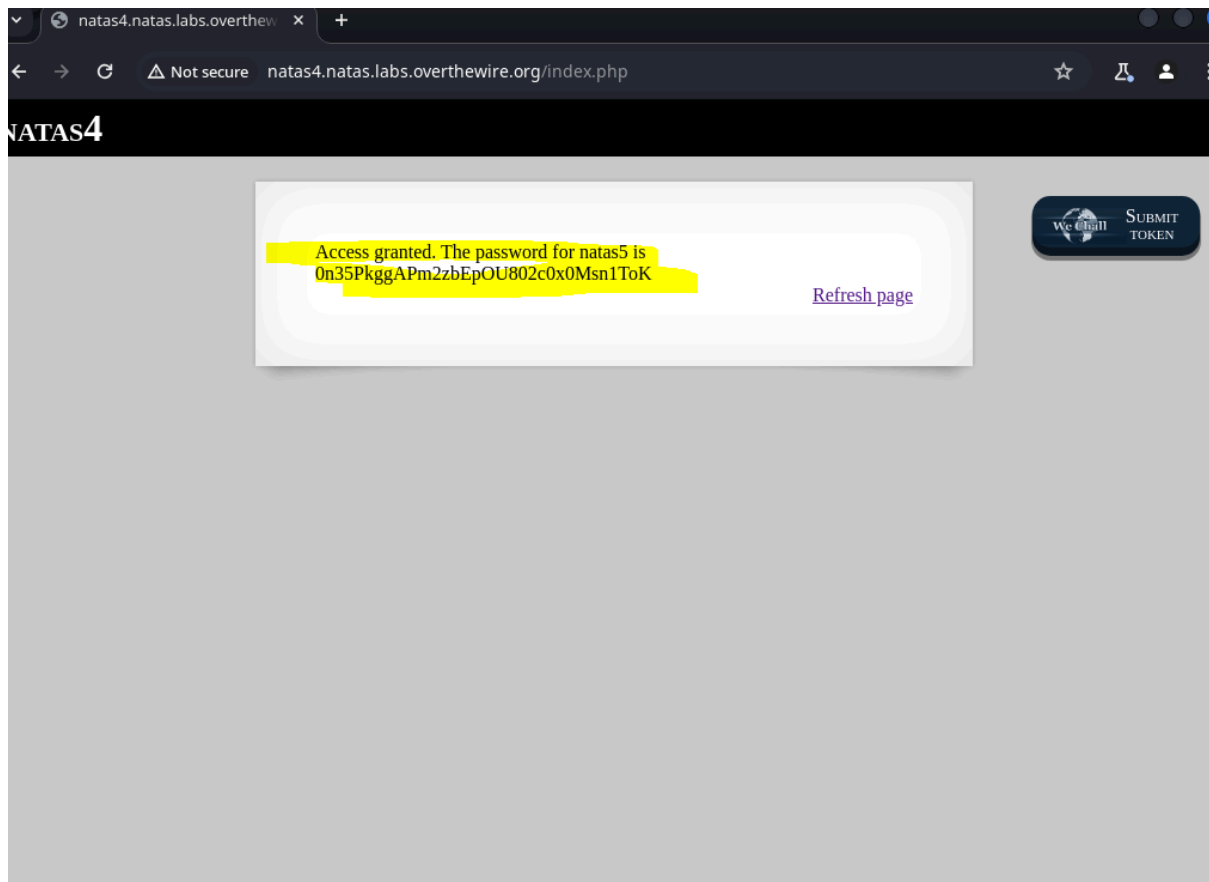
Copy and Paste the URL in the browser, and enter the username and password from the last level:



So it suggests that only users from “natas5.....” are authorized, and as we are from “natas4....” so we are blocked. We need to do something to change the link or some parameters to Natas 5 so that it will recognize us as an authorized user. This can be done if we use *Burp Suite* to change the referrer to natas5:



Open the burp suite browser paste the link of natas4, and enter the username and password from the last level. In the Burp, keep the *intercept on* changing the referrer to “natas5”, and just forward the request.



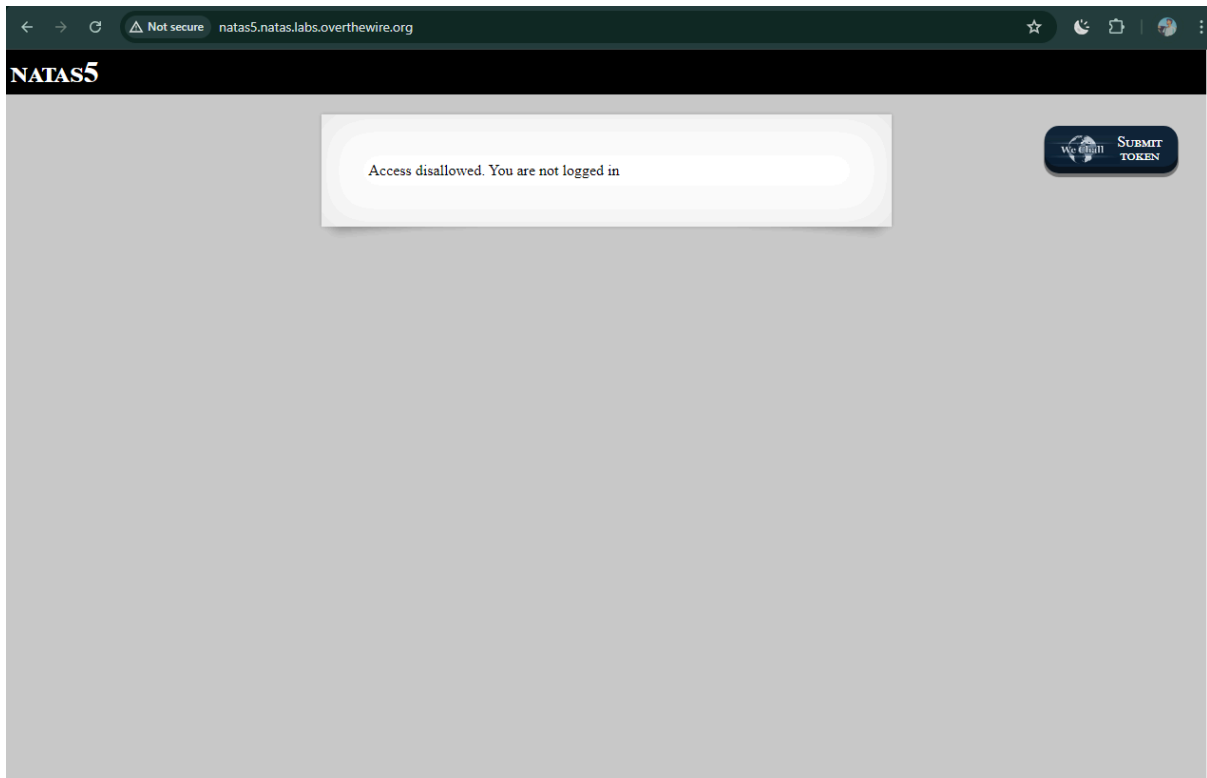
**Access granted.** The password for natas5 is  
**0n35PkggAPm2zbEpOU802c0x0Msn1ToK**

## Level 4 → Level 5:

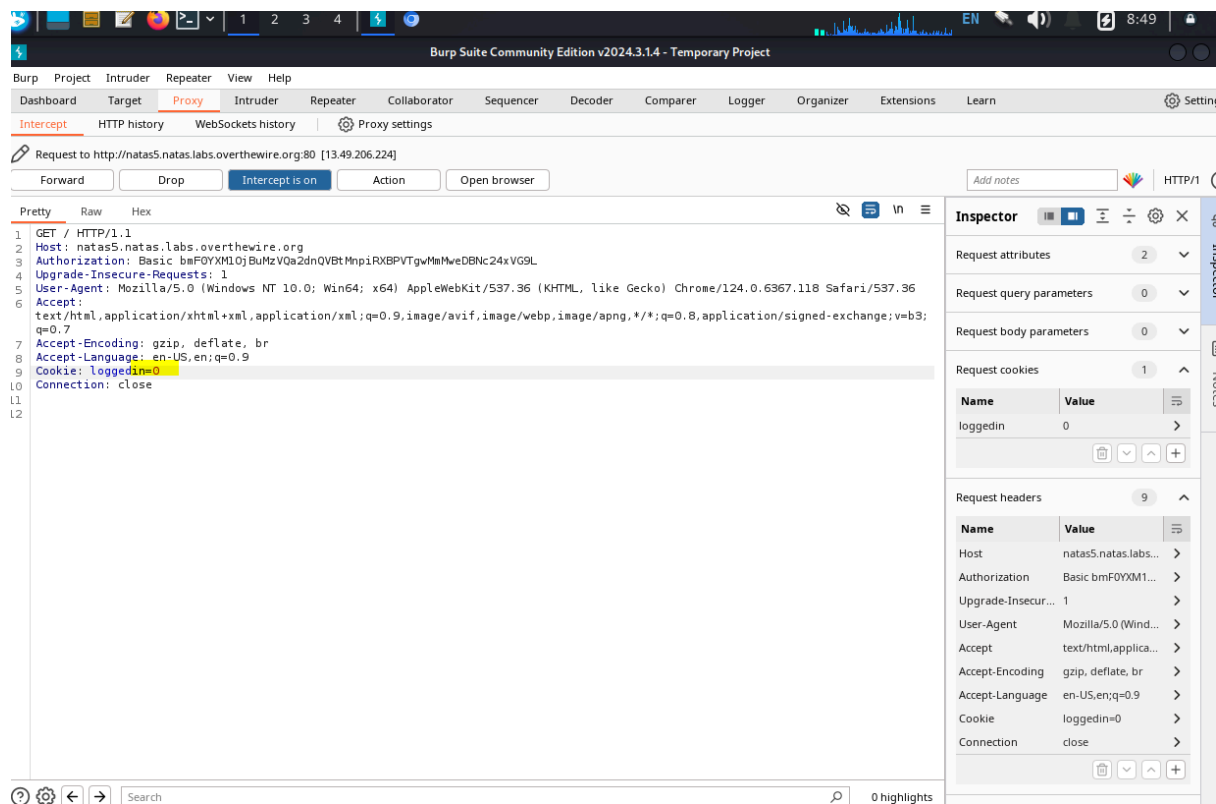
**Username: natas5**

**URL: http://natas5.natas.labs.overthewire.org**

Go to the URL and enter the username and password:



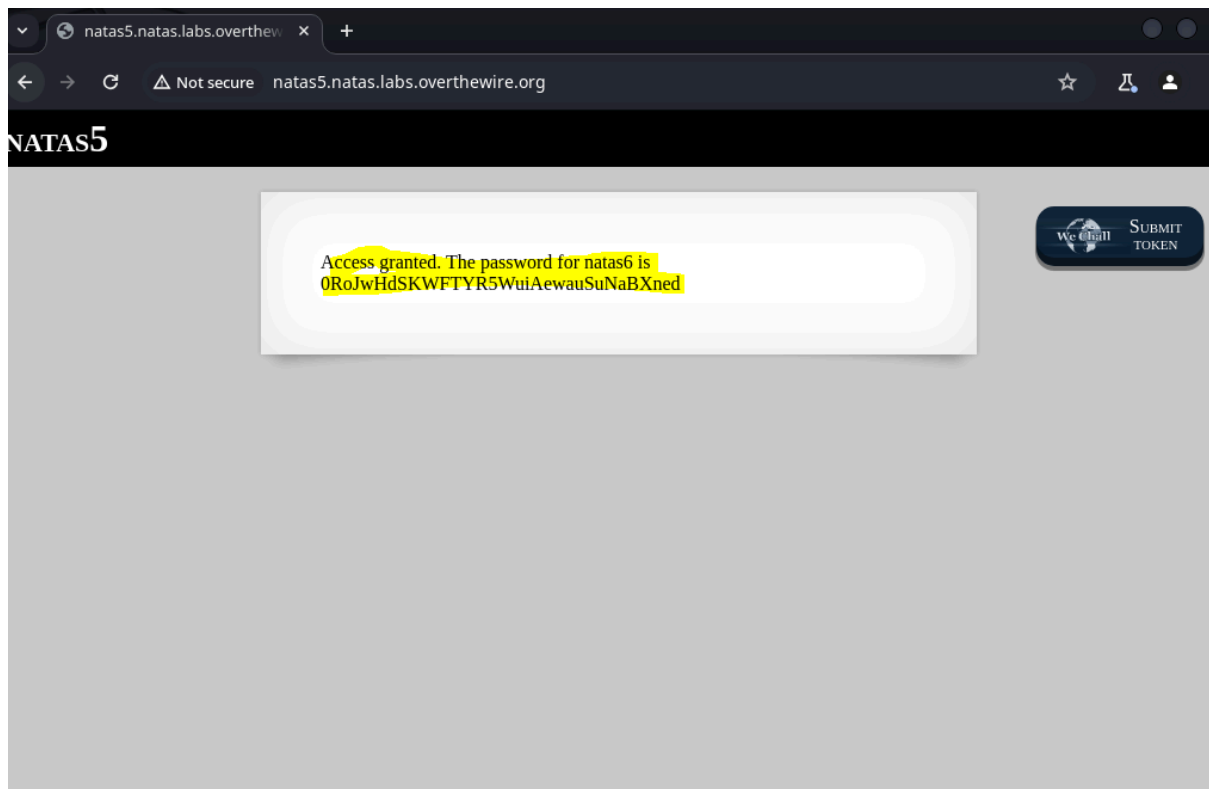
It suggests that we are not logged in. Let's check what's going on, from Burp Suite:



So here login status is set to 0, What if we set it to 1? Let's try it:

```
GET / HTTP/1.1
Host: natas5.natas.labs.overth
Authorization: Basic bmFOYXM1C
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windo
Accept:
text/html,application/xhtml+xml
q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.
Cookie: loggedin=1
Connection: close
```

And forward the request:

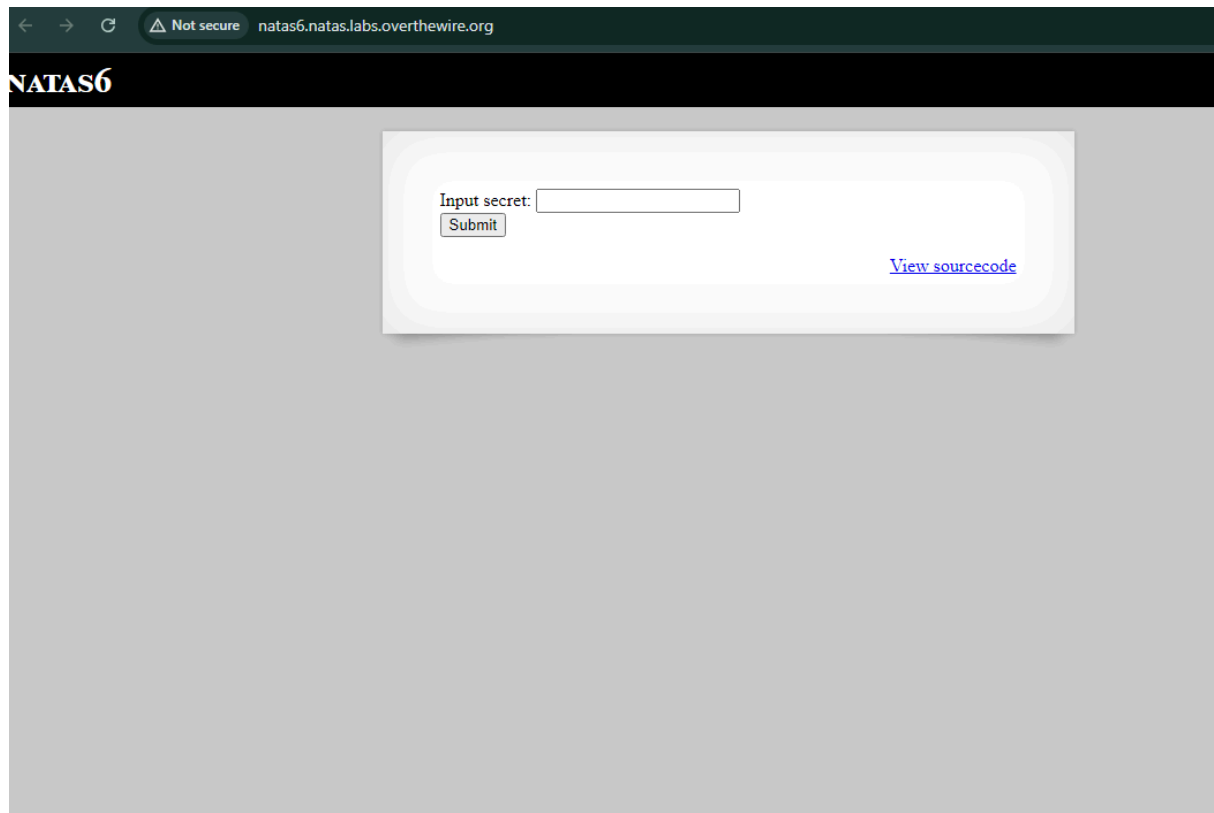


**Access granted.** The password for natas6 is  
**0RoJwHdSKWFTYR5WuiAewauSuNaBXned**

## Level 5 → Level 6:

**Username: natas6**

**URL: http://natas6.natas.labs.overthewire.org**



Go to [View Sourcecode:](#)

```

<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.
<script>var wechallinfo = { "level": "natas6", "pass": "<censored>" };</script></head>
<body>
<h1>natas6</h1>
<div id="content">

<?
include "includes/secret.inc";

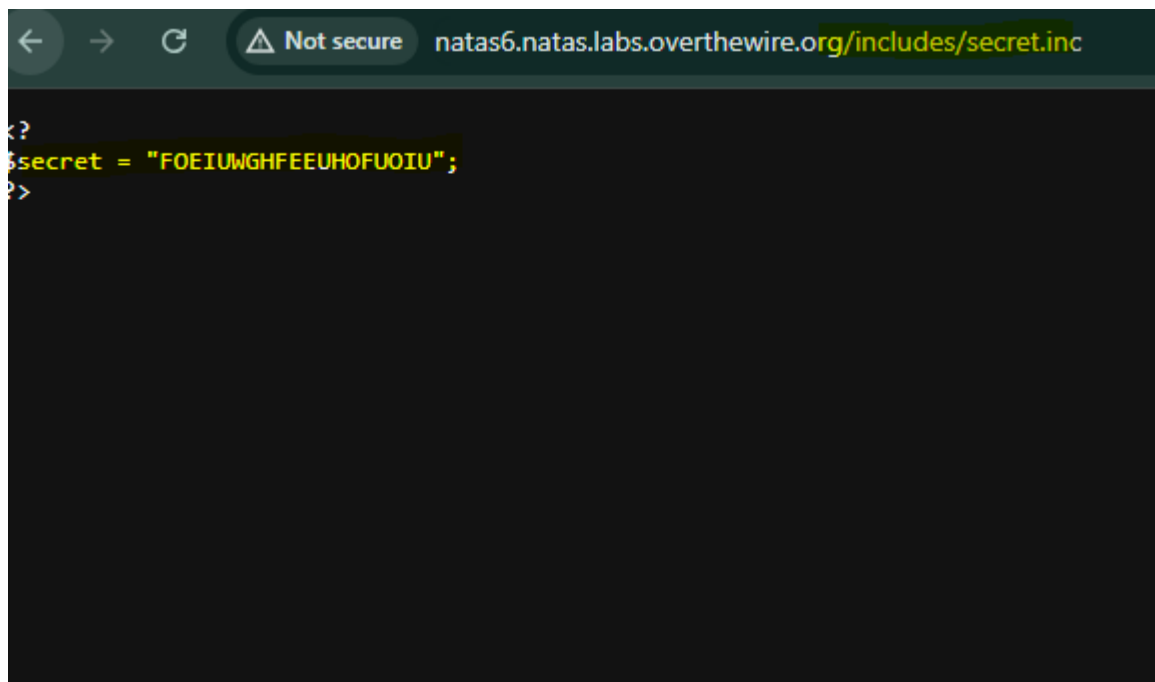
    if(array_key_exists("submit", $_POST)) {
        if($secret == $_POST['secret']) {
            print "Access granted. The password for natas7 is <censored>";
        } else {
            print "Wrong secret";
        }
    }
?>

<form method=post>
Input secret: <input name=secret><br>
<input type=submit name=submit>
</form>

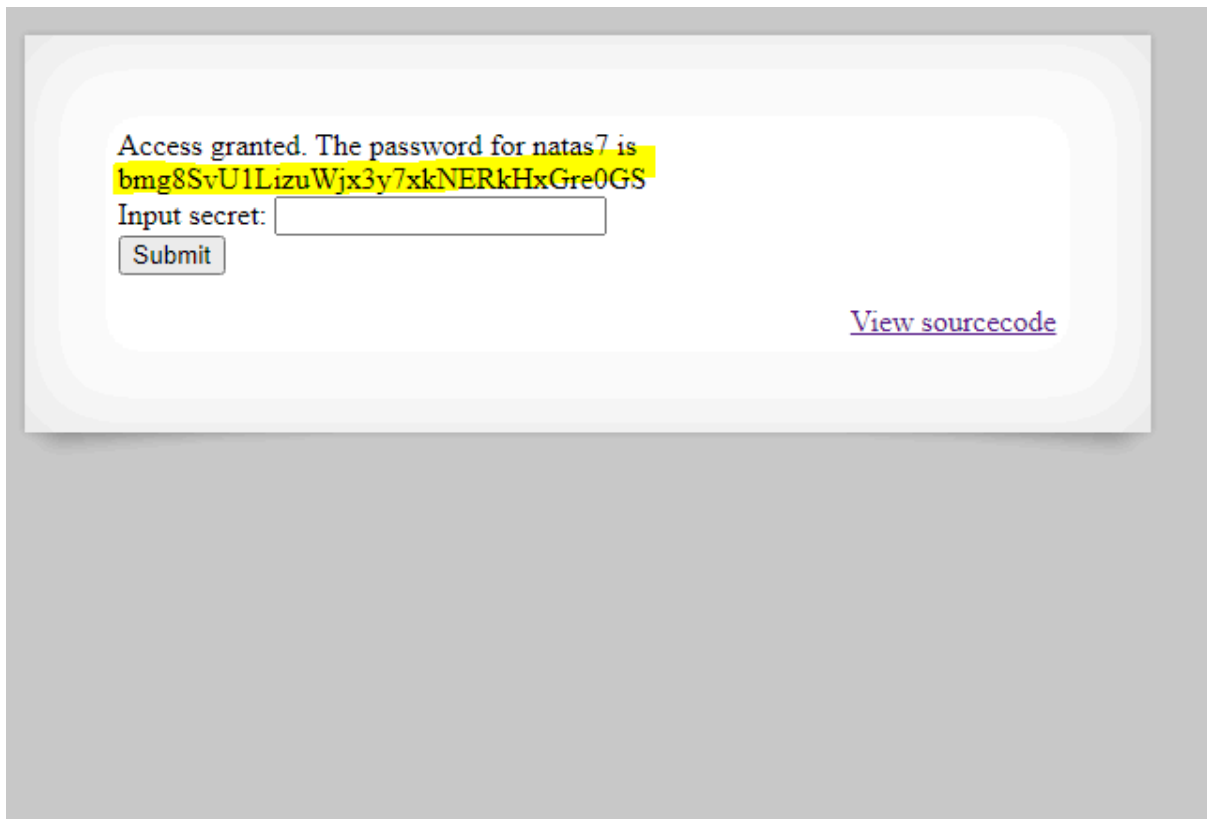
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>

```

So if we add this index to our URL:



Copy and Paste this secret to input and submit:



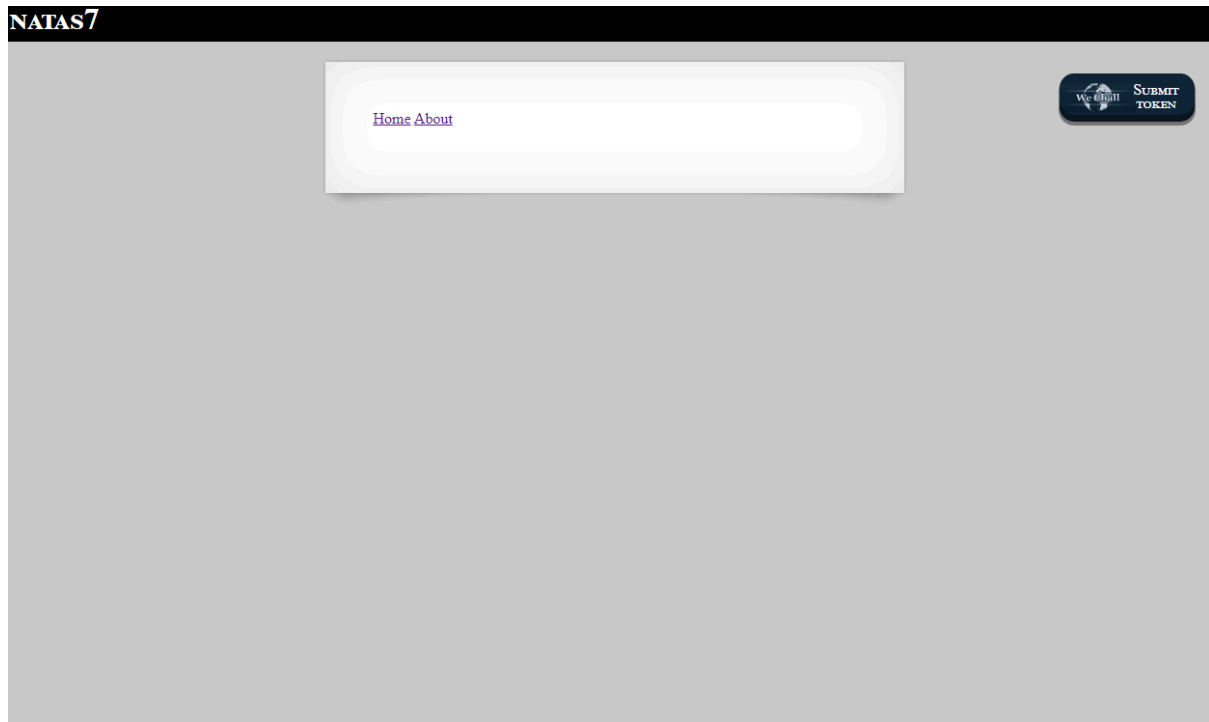
**Access granted.** The password for natas7 is  
**bmg8SvU1LizuWjx3y7xkNERkHxGre0GS**

## Level 6 → Level 7:

**Username: natas7**

**URL: http://natas7.natas.labs.overthewire.org**

After entering credentials:



So I check the source on all those 3 pages (main, home, and about) and this green line exists on all pages:

```
Line wrap ☐
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
10 <script>var wechallinfo = { "level": "natas7", "pass": "bmG8SvU1LizuWjx3y7xkNERkHxGre0GS" };</script></head>
11 <body>
12 <h1>natas7</h1>
13 <div id="content">
14
15 <a href="index.php?page=home">Home</a>
16 <a href="index.php?page=about">About</a>
17 <br>
18 <br>
19 this is the about page
20
21 <!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
22 </div>
23 </body>
24 </html>
25
```

<!-- hint: password for webuser natas8 is in /etc/natas\_webpass/natas8 →

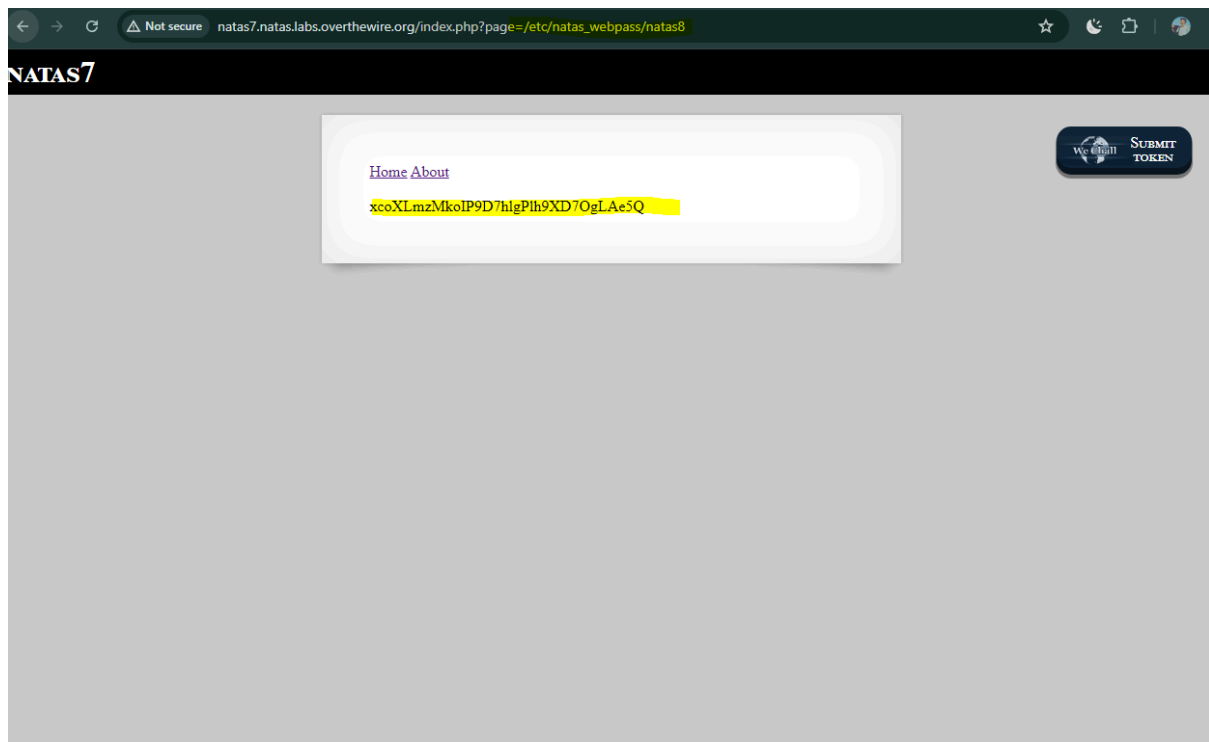
Let's add this path to the URL:

http://natas7.natas.labs.overthewire.org/index.php?page=about

To

http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas\_webpass/natas8



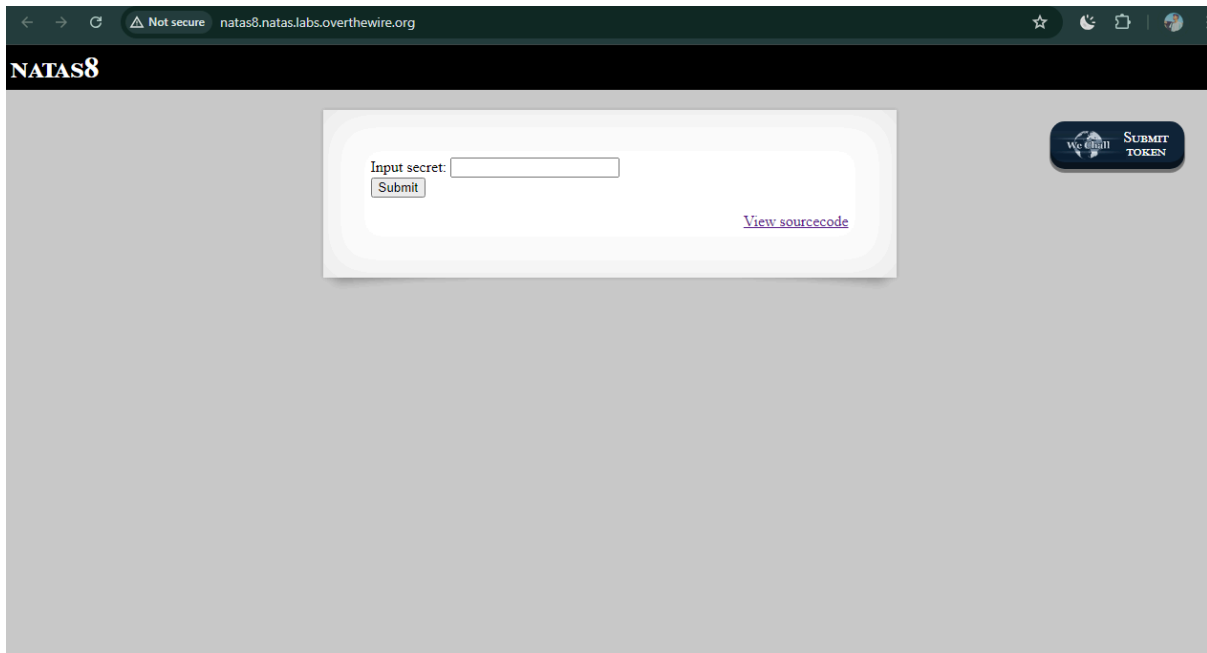


We got it: **xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q**

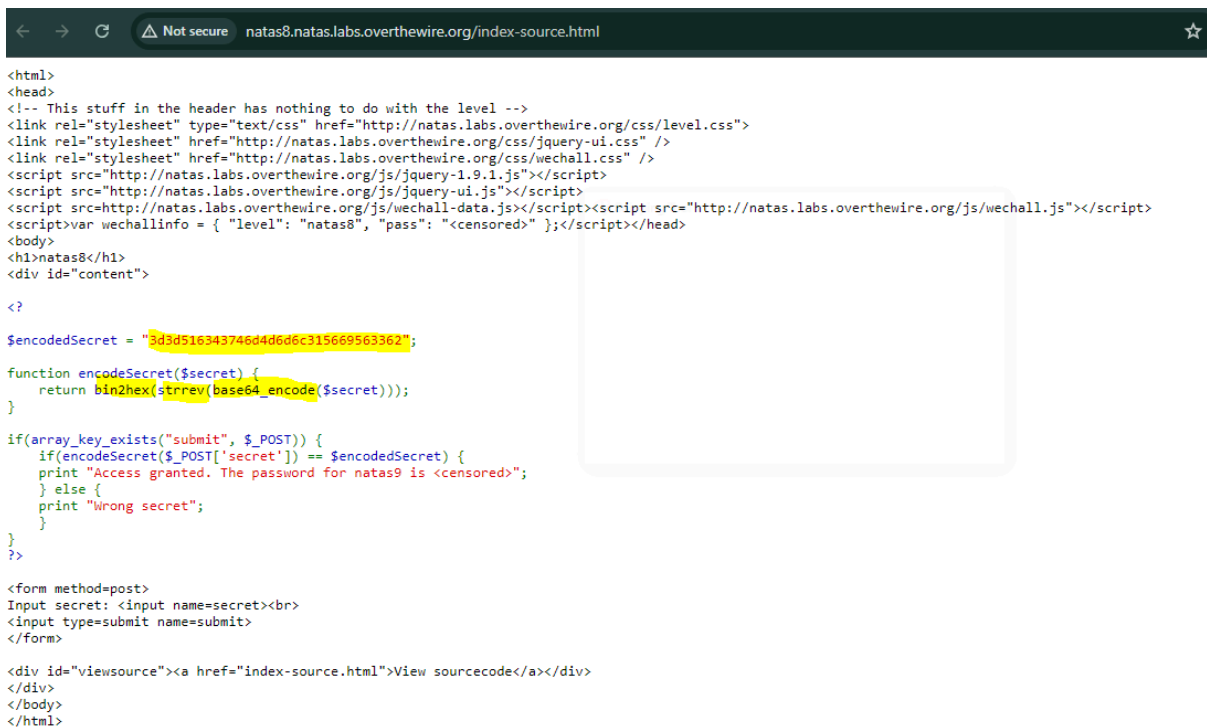
## Level 7 → Level 8:

Username: **natas8**

URL: **http://natas8.natas.labs.overthewire.org**



So It only has an Input option, submit button and source code view option. Let's see what is inside the source code:



There is an encoded text with order:

- **base64\_decode** - Decodes a string that was previously encoded with base64.
- **strrev** - Reverses the order of characters in a string.
- **hex2bin** - Converts a string of hexadecimal characters into a binary string.

While using PHP in Linux we'll use steps to crack this string:

```
(anyway@anyway)-[~]  
$ php -a  
Interactive shell  
  
php > echo base64_decode(strrev(hex2bin('3d3d516343746d4d6d6c315669563362')));  
oubWYf2kBq  
php > █
```

php -a

echo

```
base64_decode(strrev(hex2bin('3d3d516343746d4d6d6c315669563362'  
'')));
```

We got the password in the result: oubWYf2kBq


Paste the password in the input:

**NATAS8**

Access granted. The password for natas9 is  
**ZE1ck82lmdGIoEr1hQgWND6j2Wzz6b6t**

Input secret:

[View sourcecode](#)

 **SUBMIT  
TOKEN**

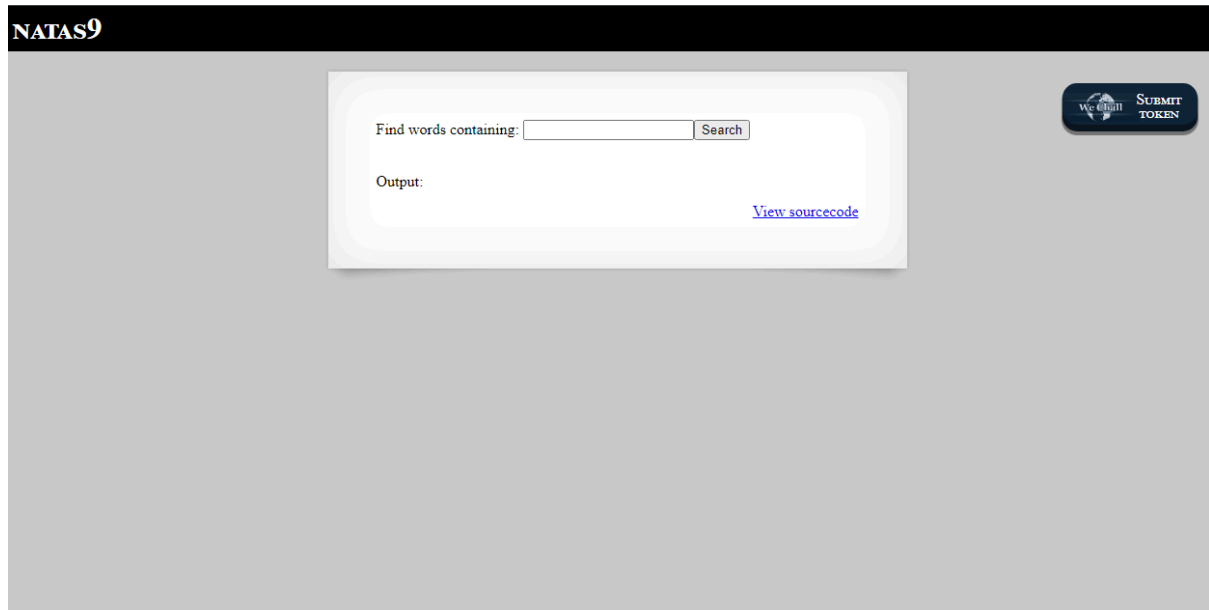
**Access granted.** The password for natas9 is  
**ZE1ck82lmdGIoEr1hQgWND6j2Wzz6b6t**

# Level 8 → Level 9:

Username: **natas9**

URL: **http://natas9.natas.labs.overthewire.org**

Going to link and entering credentials.



When we enter something, it prints every word in its dictionary that matches that input. We got to know about the dictionary because source code reveals it:

```
← → ↻ 🔒 Not secure natas9.natas.labs.overthewire.org/index-source.html 🔍 ☆

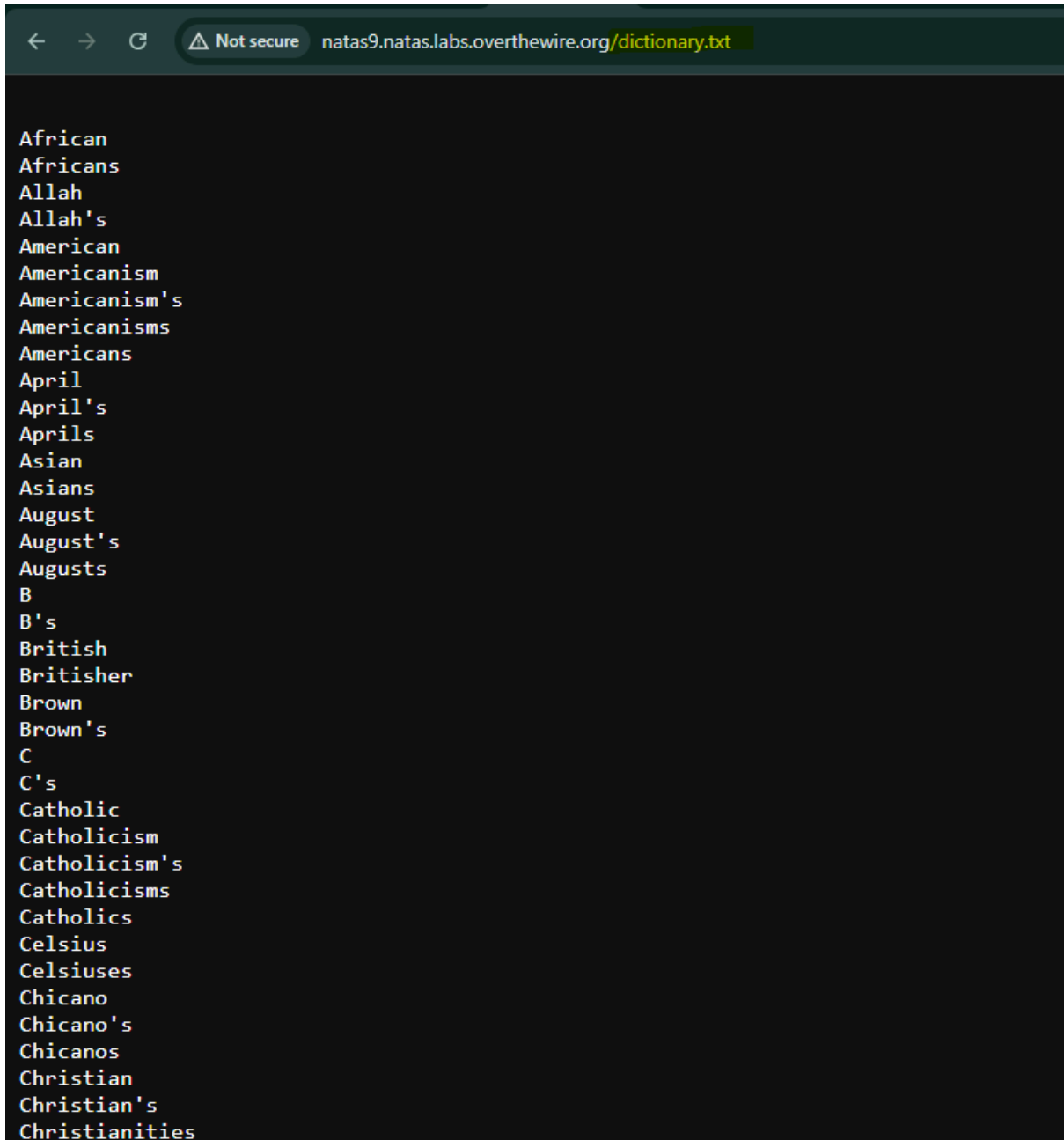
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/
</script>
<script>var wechallinfo = { "level": "natas9", "pass": "<censored>" };</script></head>
<body>
<h1>natas9</h1>
<div id="content">
<form>
Find words containing: <input name="needle"><input type="submit" name="submit" value="Search"><br><br>
</form>

Output:
<pre>
<?
$key = "";

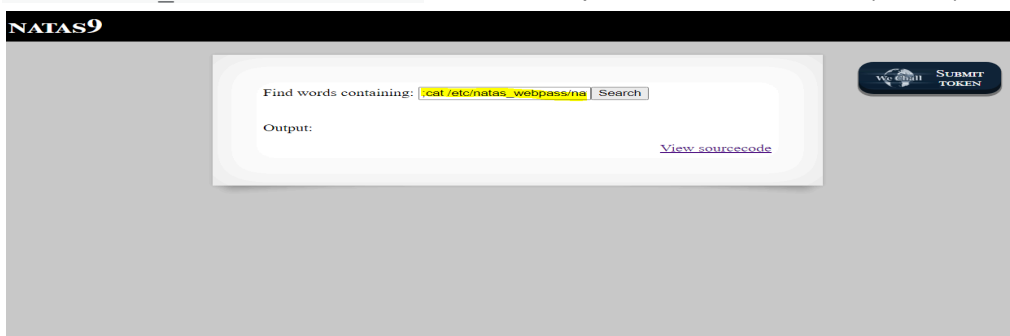
if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

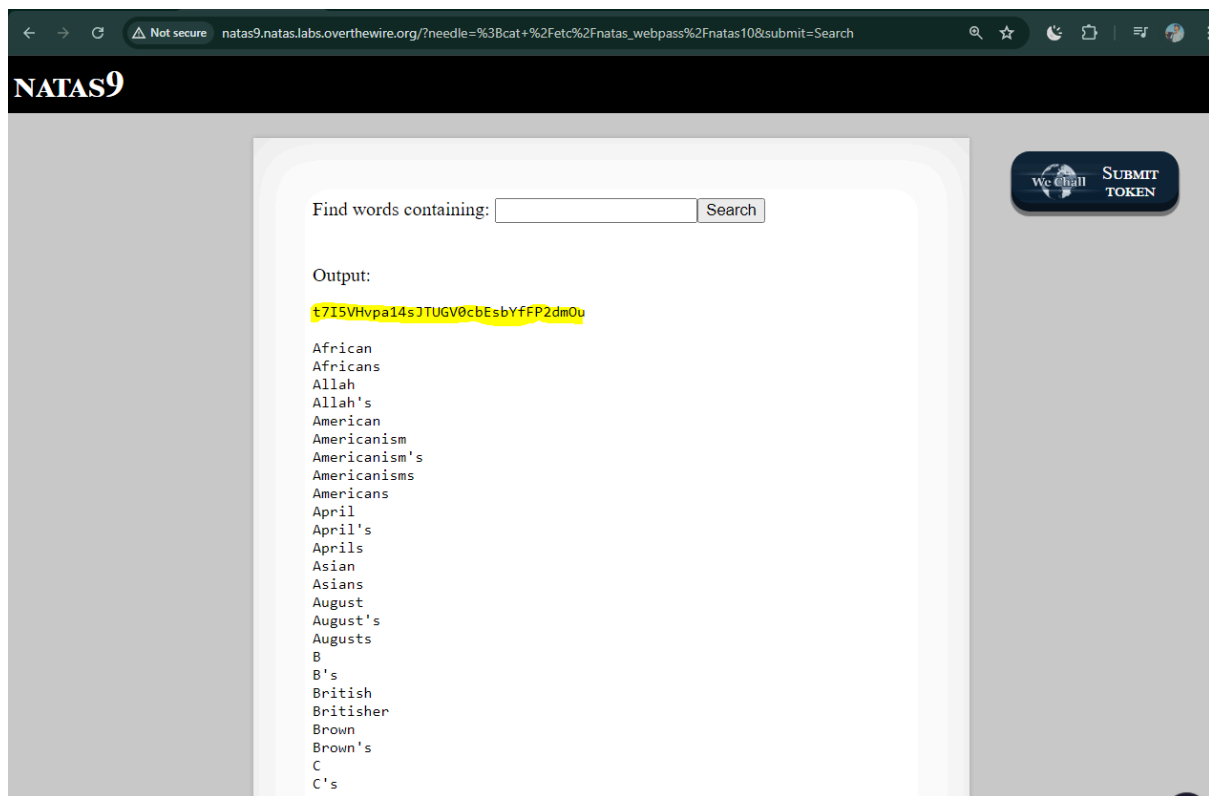
if($key != "") {
    passthru("grep -i $key dictionary.txt");
}
?>
</pre>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```



But there's a problem, it only contains the passwords of this level and we need the password (flag) of the next level (level 10). After a little research, I got to know that if we print out this path `/etc/natas_webpass/natas10`, we will have passwords for this level (level 9):



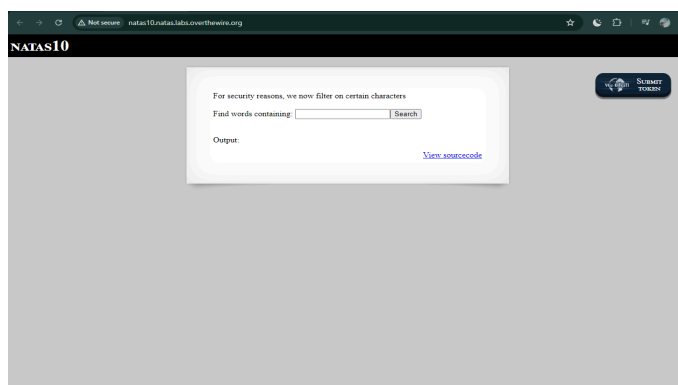


Output: **t7I5VHvpa14sJTUGV0cbEsbyfFP2dmOu**

## Level 9 → Level 10:

**Username: natas10**

**URL: http://natas10.natas.labs.overthewire.org**



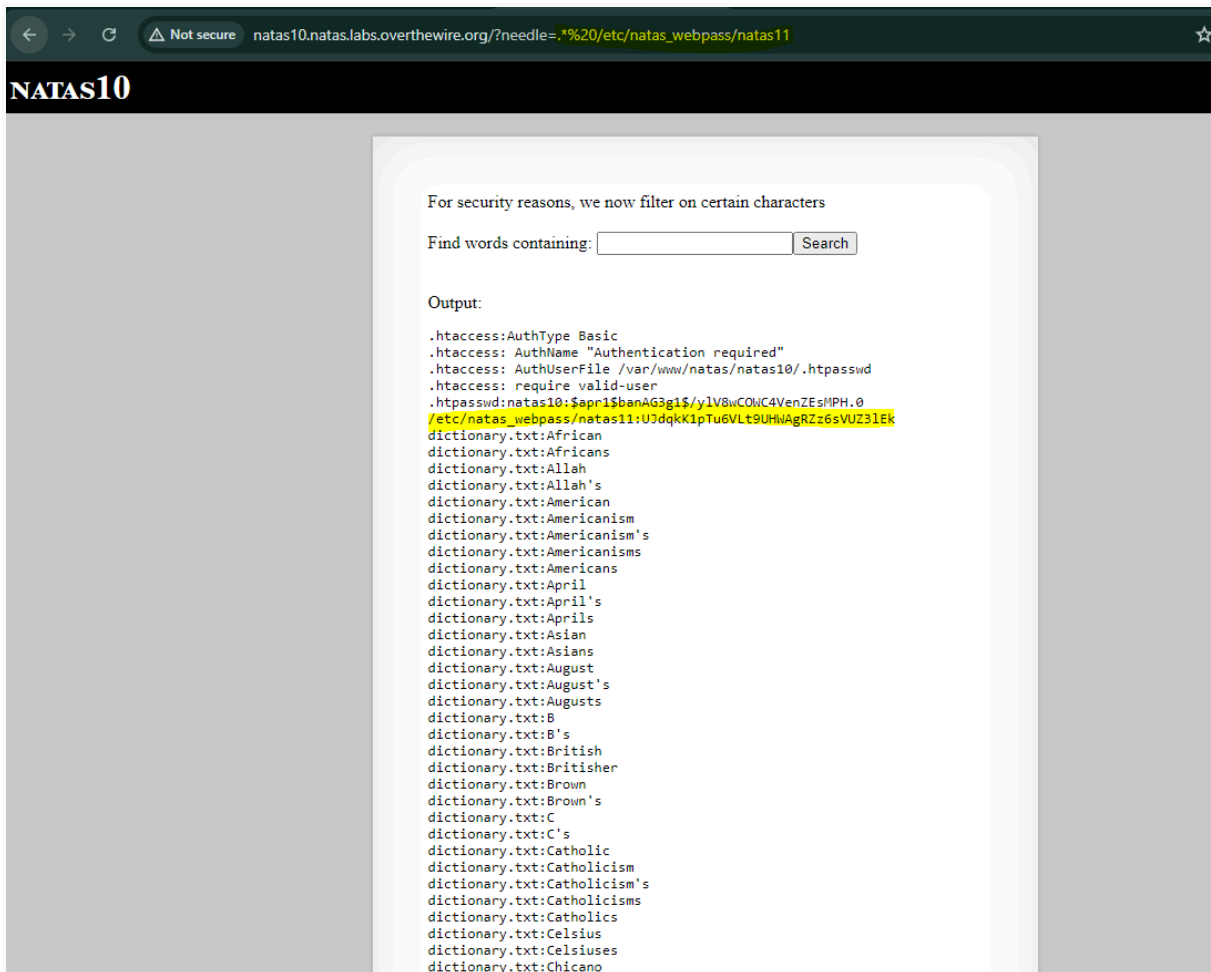
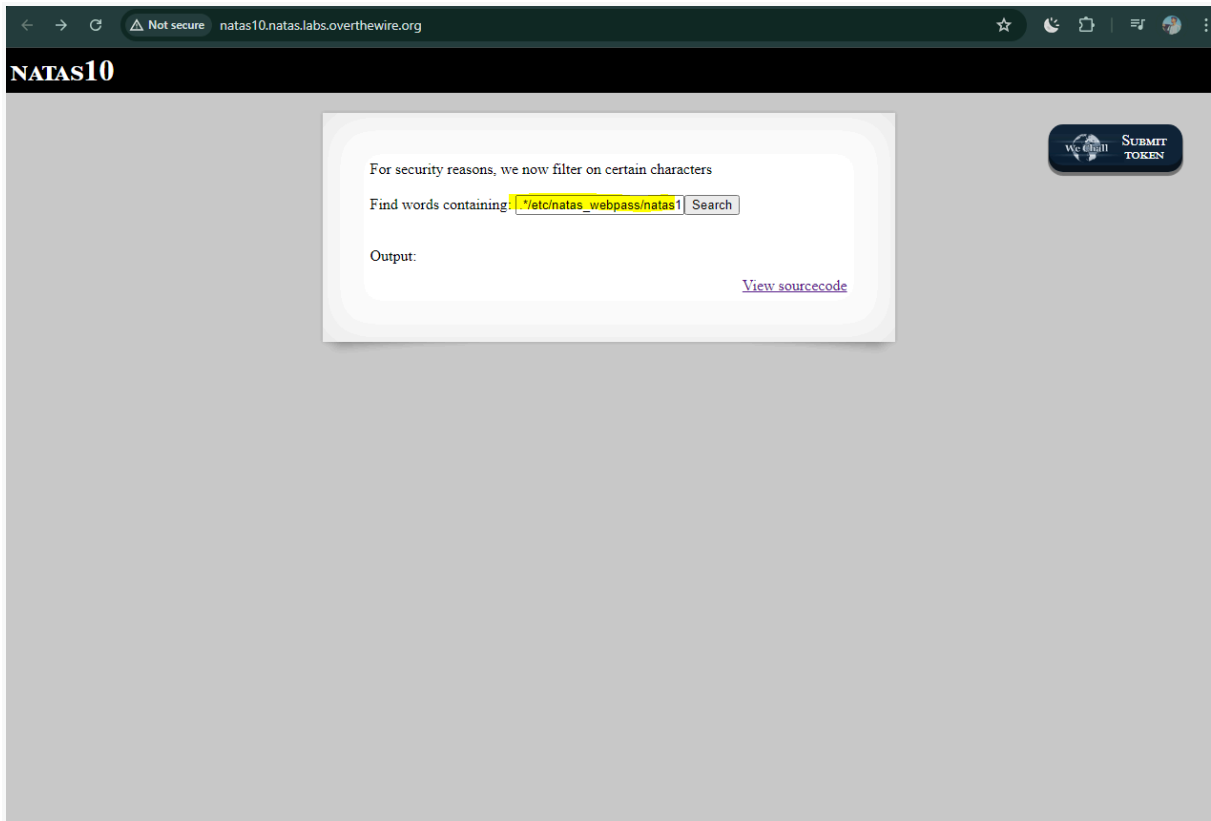
That's the same task we did before but with some changes.

```
← → ↻ ⚠ Not secure natas10.natas.labs.overthewire.org/index-source.html ☆ 🌙 📄  
  
<html>  
<head>  
<!-- This stuff in the header has nothing to do with the level -->  
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">  
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />  
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />  
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>  
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>  
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>  
<script>var wechallinfo = { "level": "natas10", "pass": "<censored>" };</script></head>  
<body>  
<h1>natas10</h1>  
<div id="content">  
  
For security reasons, we now filter on certain characters<br/><br/>  
<form>  
Find words containing: <input name="needle"><input type="submit" name="submit" value="Search"><br/><br/>  
</form>  
  
Output:  
<pre>  
<?>  
$key = "";  
  
if(array_key_exists("needle", $_REQUEST)) {  
    $key = $_REQUEST["needle"];  
}  
  
if($key != "") {  
    if(preg_match('/[;|&]', $key)) {  
        print "Input contains an illegal character!";  
    } else {  
        passthru("grep -i $key dictionary.txt");  
    }  
}  
>>  
</pre>  
  
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>  
</div>  
</body>  
</html>
```

Source code reveals that these `/ [ ; | & ] /` characters are illegal to enter.

But it works the same if we add `(*)` this character before to last input:

```
.* /etc/natas_webpass/natas11
```





We got it: **UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk**

And that's it we got all 10 flags for this task.